The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0

- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9

- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

| High Vulnerabilities | | | | |
|---|---|---|---|---|
| Primary<br>Vendor -- Product | Description | Discovered<br>Published | CVSS<br>Score | Source &<br>Patch Info |
| Aspindir -- meto_forum | Multiple SQL injection vulnerabilities in Meto Forum 1.1 allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to (a) admin/duzenle.asp and (b) admin_oku.asp; the (2) kid parameter to (c) kategori.asp and (d) admin_kategori.asp; and unspecified parameters to (e) uye.asp and (f) oku.asp. | unknown<br>2008-05-27 | 7.5 | CVE-2008-2448<br>MILW0RM<br>BID<br>BID |
| badongo -- campus_bulletin_board | Multiple SQL injection vulnerabilities in Campus Bulletin Board 3.4 allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to post3/view.asp and the (2) review parameter to post3/book.asp. | unknown<br>2008-05-28 | 7.5 | CVE-2008-2492<br>BUGTRAQ<br>BID |
| bitmixsoft -- php-jokesite | SQL injection vulnerability in jokes_category.php in PHP-Jokesite 2.0 allows remote attackers to execute arbitrary SQL commands via the cat_id parameter. | unknown<br>2008-05-27 | 7.5 | CVE-2008-2457<br>MILW0RM<br>BID |
| CaLogic -- CaLogic Calendars | SQL injection vulnerability in userreg.php in CaLogic Calendars 1.2.2 allows remote attackers to execute arbitrary SQL commands via the langsel parameter. | unknown<br>2008-05-27 | 7.5 | CVE-2008-2444<br>MILW0RM<br>BID |
| Cerulean Studios -- Trillian | Stack-based buffer overflow in Cerulean Studios Trillian before 3.1.10.0 allows remote attackers to execute arbitrary code via unspecified attributes in the X-MMS-IM-FORMAT header in an MSN message. | unknown<br>2008-05-23 | 9.3 | CVE-2008-2409<br>BID<br>SECTRACK<br>XF |

| | | | | |
|---|---|---|---|---|
| ceruleanstudios -- trillian | Stack-based buffer overflow in AIM.DLL in Cerulean Studios Trillian before 3.1.10.0 allows user-assisted remote attackers to execute arbitrary code via a long attribute value in a FONT tag in a message. | unknown 2008-05-23 | 9.3 | CVE-2008-2407 BUGTRAQ OTHER-REF SECTRACK XF |
| ceruleanstudios -- trillian_pro | Heap-based buffer overflow in the XML parsing functionality in talk.dll in Cerulean Studios Trillian Pro before 3.1.10.0 allows remote attackers to execute arbitrary code via a malformed attribute in an IMG tag. | unknown 2008-05-23 | 10.0 | CVE-2008-2408 BUGTRAQ OTHER-REF SECTRACK XF |
| Cisco -- CiscoWorks Common Services | Unspecified vulnerability in Cisco CiscoWorks Common Services 3.0.3 through 3.1.1 allows remote attackers to execute arbitrary code on a client machine via unknown vectors. | unknown 2008-05-29 | 9.3 | CVE-2008-2054 CISCO |
| comicshout -- comicshout | SQL injection vulnerability in index.php in ComicShout 2.5 and earlier allows remote attackers to execute arbitrary SQL commands via the comic_id parameter. | unknown 2008-05-27 | 7.5 | CVE-2008-2456 MILW0RM OTHER-REF BID XF |
| cPanel -- cPanel | ** DISPUTED ** scripts/wwwacct in cPanel 11.18.6 STABLE and earlier and 11.23.1 CURRENT and earlier allows remote authenticated users with reseller privileges to execute arbitrary code via shell metacharacters in the Email address field (aka Email text box). NOTE: the vendor disputes this, stating "I'm unable to reproduce such an issue on multiple servers running different versions of cPanel." | unknown 2008-05-28 | 9.0 | CVE-2008-2478 BUGTRAQ BUGTRAQ BID SECTRACK XF |
| creative -- creative_software_autoupdate_engine | Stack-based buffer overflow in the Creative Software AutoUpdate Engine ActiveX control in CTSUEng.ocx allows remote attackers to execute arbitrary code via a long CacheFolder property value. | unknown 2008-05-29 | 9.3 | CVE-2008-0955 MILW0RM CERT-VN |
| e107coders -- e107_blog_engine | SQL injection vulnerability in comment.php in the MacGuru BLOG Engine plugin 2.2 for e107 allows remote attackers to execute arbitrary SQL commands via the rid parameter. | unknown 2008-05-27 | 7.5 | CVE-2008-2455 MILW0RM BID XF |
| EMC Corporation -- AlphaStor | robotd in the Library Manager in EMC AlphaStor 3.1 SP1 for Windows allows remote attackers to execute arbitrary commands via an unspecified string field in a packet to TCP port 3500. | unknown 2008-05-29 | 10.0 | CVE-2008-2157 IDEFENSE SECTRACK |
| EMC Corporation -- AlphaStor | Multiple stack-based buffer overflows in the Command Line Interface process in the Server Agent in EMC AlphaStor 3.1 SP1 for Windows allow remote attackers to execute arbitrary code via crafted TCP packets to port 41025. | unknown 2008-05-29 | 10.0 | CVE-2008-2158 IDEFENSE SECTRACK |

| | | | | |
|---|---|---|---|---|
| Emule -- emule_plus | Unspecified vulnerability in eMule Plus before 1.2d has unknown impact and attack vectors related to "staticservers.dat processing." | unknown 2008-05-28 | 10.0 | CVE-2008-2486 OTHER-REF BID XF |
| Emule -- X_Ray | Unspecified vulnerability in the web server in eMule X-Ray before 1.4 allows remote attackers to trigger memory corruption via unknown attack vectors. | unknown 2008-05-29 | 7.5 | CVE-2008-2502 OTHER-REF |
| Excuse Online -- Excuse Online | SQL injection vulnerability in pwd.asp in Excuse Online allows remote attackers to execute arbitrary SQL commands via the pID parameter. | unknown 2008-05-29 | 7.5 | CVE-2008-2509 BUGTRAQ OTHER-REF BID XF |
| fichive -- fichive | SQL injection vulnerability in index.php in FicHive 1.0 allows remote attackers to execute arbitrary SQL commands via the letter parameter in a Search action, a different vector than CVE-2008-2416. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | unknown 2008-05-23 | 7.5 | CVE-2008-2425 |
| Henning Stoverud -- PHPhotoalbum | Multiple SQL injection vulnerabilities in PHPhotoalbum 0.5 allow remote attackers to execute arbitrary SQL commands via the (1) album parameter to thumbnails.php and the (2) pid parameter to displayimage.php. | unknown 2008-05-29 | 7.5 | CVE-2008-2501 MILW0RM XF |
| Hotscripts -- ablespace | SQL injection vulnerability in adv_cat.php in AbleSpace 1.0 allows remote attackers to execute arbitrary SQL commands via the cat_id parameter. | unknown 2008-05-28 | 7.5 | CVE-2008-2491 BUGTRAQ BID |
| icdevgroup -- interchange | Unspecified vulnerability in the 404 error page for the "Standard demo" in Interchange before 5.6.0 has unknown impact and attack vectors. | unknown 2008-05-23 | 10.0 | CVE-2008-2424 OTHER-REF |
| insanevisions -- onecms | Directory traversal vulnerability in install_mod.php in insanevisions OneCMS 2.5 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the load parameter in a go action. | unknown 2008-05-28 | 7.5 | CVE-2008-2482 BUGTRAQ MILW0RM BID XF |
| Interchange Development Group -- Interchange | Unspecified vulnerability in Interchange before 5.6.0 allows remote attackers to cause an denial of service via crafted HTTP requests. NOTE: this might be overlap CVE-2007-2635. | unknown 2008-05-23 | 10.0 | CVE-2008-2423 OTHER-REF |
| Joomla -- com_xsstream-dm | SQL injection vulnerability in the xsstream-dm (com_xsstream-dm) component 0.01 Beta for Joomla! allows remote attackers to execute arbitrary SQL commands via the movie parameter to index.php. | unknown 2008-05-27 | 7.5 | CVE-2008-2454 BUGTRAQ MILW0RM BID |

| | | | | |
|---|---|---|---|---|
| mambo-foundation -- mambo | Multiple SQL injection vulnerabilities in index.php in Mambo before 4.6.4, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) articleid and (2) mcname parameters. NOTE: some of these details are obtained from third party information. | unknown 2008-05-28 | 7.5 | CVE-2008-2498 |
| maxsite -- maxsite | SQL injection vulnerability in index.php in MAXSITE 1.10 and earlier allows remote attackers to execute arbitrary SQL commands via the category parameter in a webboard action. | unknown 2008-05-28 | 7.5 | CVE-2008-2487 MILW0RM |
| mx-system -- mxbb_portal | SQL injection vulnerability in index.php in MxBB (aka MX-System) Portal 2.7.3 allows remote attackers to execute arbitrary SQL commands via the page parameter. | unknown 2008-05-28 | 7.5 | CVE-2008-2477 MILW0RM BID |
| mytipper -- zogo_shop | SQL injection vulnerability in products.php in the Mytipper ZoGo-shop plugin 1.15.5 and 1.16 Beta 13 for e107 allows remote attackers to execute arbitrary SQL commands via the cat parameter. | unknown 2008-05-27 | 7.5 | CVE-2008-2447 MILW0RM BID XF |
| nctsoft -- NCTAudioeditor_activeX_control | Multiple stack-based buffer overflows in the Online Media Technologies NCTSoft NCTAudioGrabber2 ActiveX control in NCTAudioGrabber2.dll allow remote attackers to execute arbitrary code via unspecified vectors. | unknown 2008-05-29 | 9.3 | CVE-2008-0958 CERT-VN XF |
| netious -- netious_cms | SQL injection vulnerability in index.php in Netious CMS 0.4 allows remote attackers to execute arbitrary SQL commands via the pageid parameter, a different vector than CVE-2006-4047. | unknown 2008-05-27 | 7.5 | CVE-2008-2461 MILW0RM |
| pancake -- zina | Directory traversal vulnerability in index.php in Zina 1.0 RC3 allows remote attackers to have an unknown impact via a .. (dot dot) in the p parameter. | unknown 2008-05-28 | 7.5 | CVE-2008-2495 BUGTRAQ BID |
| phpclassifiedsscript -- php_classifieds_script | Multiple SQL injection vulnerabilities in PHP Classifieds Script allow remote attackers to execute arbitrary SQL commands via the fatherID parameter to (1) browse.php and (2) search.php. | unknown 2008-05-27 | 7.5 | CVE-2008-2453 MILW0RM BID XF |
| phpRaider -- phpRaider | PHP remote file inclusion vulnerability in authentication/phpbb3/phpbb3.functions.php in phpRaider 1.0.7 and 1.0.7a, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the pConfig_auth[phpbb_path] parameter. | unknown 2008-05-28 | 10.0 | CVE-2008-2481 MILW0RM BID |
| plusphp -- plusphp_short_url_multi-user_script | PHP remote file inclusion vulnerability in plus.php in plusPHP Short URL Multi-User Script 1.6 allows remote attackers to execute | unknown 2008-05-28 | 10.0 | CVE-2008-2480 MILW0RM BID |

| | arbitrary PHP code via a URL in the _pages_dir parameter. | | | |
|---|---|---|---|---|
| redhat -- linux_advanced_workstation<br>redhat -- Enterprise Linux Desktop<br>redhat -- enterprise_linux<br>redhat -- Enterprise Linux Desktop Workstation<br>redhat -- desktop | Buffer overflow in pattern.c in libxslt before 1.1.24 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via an XSL style sheet file with a long XSLT "transformation match" condition that triggers a large number of steps. | unknown<br>2008-05-23 | 7.5 | CVE-2008-1767<br>OTHER-REF<br>REDHAT<br>BID<br>SECTRACK<br>XF |
| Samba -- Samba | Heap-based buffer overflow in the receive_smb_raw function in util/sock.c in Samba 3.0.0 through 3.0.29 allows remote attackers to execute arbitrary code via a crafted SMB response. | unknown<br>2008-05-29 | 7.5 | CVE-2008-1105<br>BUGTRAQ<br>OTHER-REF<br>SECTRACK |
| Simpel Side -- Netbutik | Multiple SQL injection vulnerabilities in Simpel Side Netbutik 1 through 4 allow remote attackers to execute arbitrary SQL commands via the (1) cat parameter to netbutik.php and the (2) id parameter to product.php. | unknown<br>2008-05-29 | 7.5 | CVE-2008-2504<br>MILW0RM<br>BID<br>XF |
| Simpel Side -- Weblosning | Multiple SQL injection vulnerabilities in Simpel Side Weblosning 1 through 4 allow remote attackers to execute arbitrary SQL commands via the (1) mainid and (2) id parameters to index2.php. | unknown<br>2008-05-29 | 7.5 | CVE-2008-2506<br>MILW0RM<br>BID<br>XF |
| therealestatescript -- the_real_estate_script | SQL injection vulnerability in dpage.php in The Real Estate Script allows remote attackers to execute arbitrary SQL commands via the docID parameter. | unknown<br>2008-05-27 | 7.5 | CVE-2008-2443<br>MILW0RM<br>BID |
| TYPO3 -- TYPO3 | Multiple SQL injection vulnerabilities in the Statistics (aka ke_stats) extension 0.1.2 and earlier for TYPO3 allow remote attackers to execute arbitrary SQL commands via unspecified vectors. | unknown<br>2008-05-27 | 7.5 | CVE-2008-2451<br>XF |
| TYPO3 -- sg_zfelib | SQL injection vulnerability in the Library for Frontend Plugins (aka sg_zfelib) extension 1.1.512 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified "user input." | unknown<br>2008-05-28 | 7.5 | CVE-2008-2489 |
| vbulletin -- vbulletin | SQL injection vulnerability in faq.php in vBulletin 3.7.0 Gold allows remote attackers to execute arbitrary SQL commands via the q parameter in a search action. | unknown<br>2008-05-27 | 7.5 | CVE-2008-2460<br>BUGTRAQ<br>BID |
| WebSlider -- WebSlider | SQL injection vulnerability in index.php in Web Slider 0.6 allows remote attackers to execute arbitrary SQL commands via the slide parameter in a slides action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | unknown<br>2008-05-23 | 7.5 | CVE-2008-2422<br>BID<br>XF |

| wgcc -- web_group_communication_center | Multiple SQL injection vulnerabilities in Web Group Communication Center (WGCC) 1.0.3 PreRelease 1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) userid parameter to (a) profile.php in a "show moreinfo" action; the (2) bildid parameter to (b) picturegallery.php in a shownext action; the (3) id parameter to (c) filebase.php in a freigeben action, (d) schedule.php in a del action, and (e) profile.php in an observe action; and the (4) pmid parameter in a delete action and (5) folderid parameter in a showfolder action to (f) message.php. | unknown 2008-05-27 | 7.5 | CVE-2008-2446 MILW0RM BID XF |
|---|---|---|---|---|
| WordPress -- Upload File plugin | SQL injection vulnerability in wp-uploadfile.php in the Upload File plugin for WordPress allows remote attackers to execute arbitrary SQL commands via the f_id parameter. | unknown 2008-05-29 | 7.5 | CVE-2008-2510 BUGTRAQ BID |

Back to top

| Medium Vulnerabilities | | | | |
|---|---|---|---|---|
| Primary Vendor -- Product | Description | Discovered Published | CVSS Score | Source & Patch Info |
| 4shared -- starsgames_control_panel | Cross-site scripting (XSS) vulnerability in index.php in Starsgames Control Panel 4.6.2 and earlier allows remote attackers to inject arbitrary web script or HTML via the st parameter. | unknown 2008-05-27 | 4.3 | CVE-2008-2458 BUGTRAQ BID XF |
| badongo -- phpfix | Multiple SQL injection vulnerabilities in phpFix 2.0 allow remote attackers to execute arbitrary SQL commands via the (1) kind parameter to fix/browse.php and the (2) account parameter to auth/00_pass.php. | unknown 2008-05-28 | 6.8 | CVE-2008-2479 BUGTRAQ BID |
| badongo -- campus_bulletin_board | Cross-site scripting (XSS) vulnerability in post3/Book.asp in Campus Bulletin Board 3.4 allows remote attackers to inject arbitrary web script or HTML via the review parameter. | unknown 2008-05-28 | 4.3 | CVE-2008-2493 BUGTRAQ BID |
| Barracuda Networks -- Barracuda Spam Firewall | Cross-site scripting (XSS) vulnerability in ldap_test.cgi in Barracuda Spam Firewall (BSF) before 3.5.11.025 allows remote attackers to inject arbitrary web script or HTML via the email parameter. | unknown 2008-05-23 | 4.3 | CVE-2008-2333 OTHER-REF |
| beaussier -- roomphplanning | admin/userform.php in RoomPHPLanning 1.5 does not require administrative credentials, which allows remote authenticated users to create new admin accounts. | unknown 2008-05-28 | 6.5 | CVE-2008-2488 MILW0RM BID |
| Brown Bear Software -- Calcium | Cross-site scripting (XSS) vulnerability in Calcium40.pl in Brown Bear Software Calcium 3.10 and 4.0.4 allows remote attackers to inject arbitrary web script or | unknown 2008-05-29 | 4.3 | CVE-2008-2507 BUGTRAQ BID |

| | | | | |
|---|---|---|---|---|
| | HTML via the CalendarName parameter in a ShowIt action. | | | |
| Django Project -- Django | Cross-site scripting (XSS) vulnerability in the login form in the administration application in Django 0.91 before 0.91.2, 0.95 before 0.95.3, and 0.96 before 0.96.2 allows remote attackers to inject arbitrary web script or HTML via the URI of a certain previous request. | unknown 2008-05-23 | 4.3 | CVE-2008-2302 SECTRACK |
| entertainmentscript -- entertainmentscript | Directory traversal vulnerability in page.php in EntertainmentScript 1.4.0 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the page parameter. | unknown 2008-05-27 | 6.8 | CVE-2008-2459 MILW0RM BID XF |
| IBM -- Lotus Sametime | Stack-based buffer overflow in the Community Services Multiplexer (aka MUX or StMux.exe) in IBM Lotus Sametime 7.5.1 CF1 and earlier, and 8.x before 8.0.1, allows remote attackers to execute arbitrary code via a crafted URL. | unknown 2008-05-29 | 5.0 | CVE-2008-2499 OTHER-REF OTHER-REF BID |
| ikemcg -- phpinstantgallery | Multiple cross-site scripting (XSS) vulnerabilities in Isaac McGowan phpInstantGallery 2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) gallery parameter to (a) index.php and (b) image.php, and the (2) imgnum parameter to image.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | unknown 2008-05-27 | 4.3 | CVE-2008-2449 BID XF |
| Linux -- Kernel Debian -- Debian Linux | The (1) sparc_mmap_check function in arch/sparc/kernel/sys_sparc.c and the (2) sparc64_mmap_check function in arch/sparc64/kernel/sys_sparc.c, in the Linux kernel before 2.6.25.3, omit some virtual-address range (aka span) checks when the mmap MAP_FIXED bit is not set, which allows local users to cause a denial of service (panic) via unspecified mmap calls. | unknown 2008-05-29 | 4.4 | CVE-2008-2137 MLIST OTHER-REF DEBIAN BID |
| Mambo -- MostlyCE | Cross-site scripting (XSS) vulnerability in the MOStlyContent Editor (MOStlyCE) component before 3.0 for Mambo allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown 2008-05-29 | 5.0 | CVE-2008-2500 |
| mambo-foundation -- mambo | CRLF injection vulnerability in Mambo before 4.6.4 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors. | unknown 2008-05-28 | 5.0 | CVE-2008-2497 |
| Mozilla -- Firefox | Mozilla Firefox 2.0.0.14 allows remote attackers to cause a denial of service (heap corruption and application crash) or possibly execute arbitrary code by triggering an error condition during certain Iframe operations between a JSframe write and a JSframe close, as demonstrated by an error in loading an empty Java applet defined by a | unknown 2008-05-23 | 4.3 | CVE-2008-2419 OTHER-REF BID XF |

| | 'src="javascript:'" sequence. | | | |
|---|---|---|---|---|
| openssl -- openssl | Double free vulnerability in OpenSSL 0.9.8f and 0.9.8g, when the TLS server name extensions are enabled, allows remote attackers to cause a denial of service (crash) via a crafted packet. NOTE: some of these details are obtained from third party information. | unknown 2008-05-29 | 4.3 | CVE-2008-0891 OTHER-REF |
| OpenSSL Project -- OpenSSL | OpenSSL 0.9.8f and 0.9.8g allows remote attackers to cause a denial of service (crash) via a TLS handshake that omits the Server Key Exchange message and uses "particular cipher suites." | unknown 2008-05-29 | 4.3 | CVE-2008-1672 OTHER-REF |
| pancake -- zina | Cross-site scripting (XSS) vulnerability in index.php in Zina 1.0 RC3 allows remote attackers to inject arbitrary web script or HTML via the l parameter. | unknown 2008-05-28 | 4.3 | CVE-2008-2494 BUGTRAQ BID |
| PCPIN -- PCPIN Chat | Cross-site scripting (XSS) vulnerability in the URL redirection script (inc/url_redirection.inc.php) PCPIN Chat before 6.11 allows remote attackers to inject arbitrary web script or HTML via unknown vectors. | unknown 2008-05-28 | 4.3 | CVE-2008-2485 BUGTRAQ OTHER-REF BID |
| quate -- quate_cms | Multiple cross-site scripting (XSS) vulnerabilities in Quate CMS 0.3.4 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) index.php, (2) login.php, and (3) credits.php in admin/, and (4) upgrade/index.php. | unknown 2008-05-28 | 4.3 | CVE-2008-2496 MILW0RM BID XF |
| redhat -- network_satellite_server | Cross-site scripting (XSS) vulnerability in the Red Hat Network channel search feature, as used in RHN and Red Hat Network Satellite before 5.0.2, allows remote attackers to inject arbitrary web script or HTML via unknown vectors. | unknown 2008-05-23 | 4.3 | CVE-2007-5961 OTHER-REF REDHAT SECTRACK XF |
| SAP -- Web Dynpro SAP -- SAP Web Application Server | Cross-site scripting (XSS) vulnerability in the Web GUI in SAP Web Application Server (WAS) 7.0, Web Dynpro for ABAP (aka WD4A or WDA), and Web Dynpro for BSP allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to the default URI under bc/gui/sap/its/webgui/. | unknown 2008-05-23 | 4.3 | CVE-2008-2421 BUGTRAQ BID |
| selinux -- setroubleshoot | sealert in setroubleshoot 2.0.5 allows local users to overwrite arbitrary files via a symlink attack on the sealert.log temporary file. | unknown 2008-05-23 | 4.4 | CVE-2007-5495 OTHER-REF BID SECTRACK |
| Simpel Side -- Weblosninger | Cross-site scripting (XSS) vulnerability in result.php in Simpel Side Weblosning 1 through 4 allows remote attackers to inject arbitrary web script or HTML via the search parameter. | unknown 2008-05-29 | 4.3 | CVE-2008-2505 MILW0RM BID XF |

| SourceForge -- eMule X-Ray | Buffer overflow in Uploadlist in eMule X-Ray before 1.4 has unknown impact and remote attack vectors. | unknown 2008-05-29 | 6.8 | CVE-2008-2503 OTHER-REF XF |
|---|---|---|---|---|
| Stunnel -- Stunnel | The OCSP functionality in stunnel before 4.24 does not properly search certificate revocation lists (CRL), which allows remote attackers to bypass intended access restrictions by using revoked certificates. | unknown 2008-05-23 | 6.8 | CVE-2008-2420 MLIST XF |
| Sun -- Solaris | Race condition in the STREAMS Administrative Driver (sad) in Sun Solaris 10 allows local users to cause a denial of service (panic) via unknown vectors. | unknown 2008-05-23 | 4.7 | CVE-2008-2418 SUNALERT BID |
| TYPO3 -- TYPO3 | Multiple cross-site scripting (XSS) vulnerabilities in the Statistics (aka ke_stats) extension 0.1.2 and earlier for TYPO3 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown 2008-05-27 | 4.3 | CVE-2008-2450 XF |
| TYPO3 -- TYPO3 | Cross-site scripting (XSS) vulnerability in the Questionaire (aka pbsurvey) extension 1.2.0 and earlier for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown 2008-05-27 | 4.3 | CVE-2008-2452 XF |
| TYPO3 -- kj_imagelightbox2 | Cross-site scripting (XSS) vulnerability in the KJ Image Lightbox 2 (aka kj_imagelightbox2) extension 1.4.2 and earlier for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified "user input." | unknown 2008-05-28 | 4.3 | CVE-2008-2490 |
| Ussun -- Power Audio CD Grabber Orion Studios -- CinematicMP3 AliveMedia -- Alive MP3 WAV Converter Online Media Technologies -- NCTAudioStudio ActiveX control Online Media Technologies -- NCTAudioEditor ActiveX control Ussun -- Power Audio CD Burner | Multiple stack-based buffer overflows in the Online Media Technologies NCTSoft NCTAudioInformation2 ActiveX control in NCTAudioInformation2.dll allow remote attackers to execute arbitrary code via unspecified vectors. | unknown 2008-05-29 | 5.1 | CVE-2008-0959 CERT-VN XF |
| wgcc -- web_group_communication_center | Cross-site scripting (XSS) vulnerability in profile.php in Web Group Communication Center (WGCC) 1.0.3 PreRelease 1 and earlier allows remote attackers to inject arbitrary web script or HTML via the userid parameter in a show action. | unknown 2008-05-27 | 4.3 | CVE-2008-2445 MILW0RM BID XF |
| xomol -- xomol_cms | Directory traversal vulnerability in index.php in Xomol CMS 1.20071213 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the op parameter. | unknown 2008-05-28 | 6.8 | CVE-2008-2483 MILW0RM BID |
| xomol -- xomol_cms | SQL injection vulnerability in index.php in Xomol CMS 1.20071213, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the email parameter. | unknown 2008-05-28 | 6.8 | CVE-2008-2484 MILW0RM BID |

Back to top

## Low Vulnerabilities

| Primary<br>Vendor -- Product | Description | Discovered<br>Published | CVSS<br>Score | Source & Patch<br>Info |
|---|---|---|---|---|
| selinux -- setroubleshoot | Cross-site scripting (XSS) vulnerability in setroubleshoot 2.0.5 allows local users to inject arbitrary web script or HTML via a crafted (1) file or (2) process name, which triggers an Access Vector Cache (AVC) log entry in a log file used during composition of HTML documents for sealert. | unknown<br>2008-05-23 | 1.9 | CVE-2007-5496<br>OTHER-REF<br>BID |
| Tr Script News -- Tr Script News | Cross-site scripting (XSS) vulnerability in news.php in Tr Script News 2.1 allows remote attackers to inject arbitrary web script or HTML via the "nb" parameter in voir mode. | unknown<br>2008-05-29 | 2.8 | CVE-2008-2508<br>OTHER-REF<br>BID<br>XF |

Back to top